Title	ノルム・トーラスのクンマー理論 (代数的整数論とその周辺)
Author(s)	木田, 雅成
Citation	数理解析研究所講究録 (2005), 1451: 237-242
Issue Date	2005-10
URL	http://hdl.handle.net/2433/47742
Right	
Type	Departmental Bulletin Paper
Textversion	publisher

数理解析研究所講究録 1451 巻 2005 年 237-242

ノルム・トーラスのクンマー理論

木田雅成 (Kida, Masanari) *
電気通信大学
(University of Electro-Communications)

1 背景

k を体とし, m を体の標数 $\mathrm{ch}(k)$ と素な正整数で 1 より大きいとする. k は 1 の m 乗根の群 μ_m を含むと仮定すると, Kummer 列

$$1 \to \mu_m \to \bar{k}^* \xrightarrow{m\text{乗}} \bar{k}^* \to 1 \text{ (完全)}$$

から Kummer duality

$$k^*/(k^*)^n \cong \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\bar{k}/k), \mu_m)$$

が得られるというのが古典的なクンマー理論である. これを使うと k の m 次巡回拡大が具体的に簡単に書けることがわかるので, 多くの数論的な応用を持つことは周知のとおりである.

この古典的なクンマー理論を乗法群 $\mathbb{G}_m$ に関するものとしてとらえなおし, 代数群に一般化することは Lang-Tate [5] によって始められ, 本田 [1], Ribet [8] によってさらに深く研究されてきた. これらの理論も多くの応用をもつ. 代数群の有理点の計算に使われるのがその代表例である.

しかしながら, 一般の代数群の場合に上のような完全な duality を証明できる場合は少ない. 本論ではある条件の下でノルム・トーラスに対して Kummer duality が成立することをみる. これは古典的な場合の自然な拡張となっており, 多くの体についてある巡回拡大体の完全な分類を与えるものである.

二年前の本研究集会で行なわれた小川氏の講演 [6] と小松亨氏による独立した研究 [3] がこの研究の端緒となっている. そこでは円文体の最大実部分体を含むような体に対して,

* 本研究は科学研究費補助金 基盤 (C) (No. 16540014) の援助をうけています.

ある一次元代数群を使ってクンマー理論を展開しているのであるが, この研究はその高次元への拡張でもある. 本講究録に収録される諏訪紀幸氏の研究もこれらの研究の別の方向への一般化になっていることをここで注意しておく.

2 定理

K/k を体のガロア拡大とし, その次数を n とする. ノルム・トーラス $R^{(1)}_{K/k}\mathbb{G}_m$ は k 上の代数的トーラスの完全系列

$$1 \to R^{(1)}_{K/k}\mathbb{G}_m \to R_{K/k}\mathbb{G}_m \xrightarrow{N} \mathbb{G}_m \to 1 \tag{1}$$

によって定義される. ここで $N = N_{K/k}$ はノルム写像から誘導される写像である. $R^{(1)}_{K/k}\mathbb{G}_m$ は $n-1$ 次元の代数的トーラスで, その k 有理点は $\ker(N_{K/k} : K^* \to k^*)$ と同型になる. 詳しい性質については [9] を参照のこと.

定義 1. 体 k と $\mathrm{char}(k)$ と素な整数 $m \geq 2$ の組 (k, m) が Kummer 対 (Kummerian pair)[*1] であるとは $K = k(\zeta_m), n = [K : k]$ とするときに次の 4 条件をみたすことをいう.

(I) K/k は巡回拡大.
(II) m は平方因子なしで, $m = p_1 \ldots p_r$ と素因数分解した時に $p_i \equiv 1 \pmod{n}$ をみたす.
(III) $[\mathbb{Q}(\zeta_{p_i}) : k \cap \mathbb{Q}(\zeta_{p_i})] = n$ がすべての p_i について成り立つ.
(IV) 各 p_i の上にある $\mathbb{Z}[\zeta_n]$ の素イデアルは単項イデアルである.

この定義の下に次の定理が成り立つ.

定理 2. (k, m) が *Kummer* 対ならば, $R^{(1)}_{K/k}\mathbb{G}_m$ の m 次巡回自己準同型 λ があって, *Kummer duality*

$$R^{(1)}_{K/k}\mathbb{G}_m(k)/\lambda(R^{(1)}_{K/k}\mathbb{G}_m(k)) \cong \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\bar{k}/k), \ker\lambda)$$

がなりたつ.

写像は具体的に与えることができて, $x \in R^{(1)}_{K/k}\mathbb{G}_m(k)$ に対して, $\lambda(y) = x$ をみたす $y \in R^{(1)}_{K/k}\mathbb{G}_m(\bar{k})$ をとって, $\phi_x \in \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\bar{k}/k), \ker\lambda)$ を $\phi_x(\tau) = y^{\tau-1} (\tau \in \mathrm{Gal}(\bar{k}/k))$ とすればよい. この定理から特に (k, m) が Kummer 対のとき, k の m 次巡回拡大体が $R^{(1)}_{K/k}\mathbb{G}_m(k)$ の元の λ による逆像を k に添加して得られることがわかる.

ここでどのような対 (k, m) がクンマー対になるかを考察する.

[*1] 講演時から名称, 定義を少し変更した.

- m が素数ならば (I)(II)(III) は自動的に成り立つ.
- $n < 23$ なら $\mathbb{Z}[\zeta_n]$ は単項イデアル整域なので (IV) は成り立つ[*2]

これから素円分体の大きな部分体とその導手の組はクンマー対になる. 一般には, n を固定した時, 円分体 $\mathbb{Q}(\zeta_m)$ の部分体 k で $[K : k] = n$ をみたすもののうち, (k, m) が Kummer 対になるものは m の素因子の個数が多くなるとともにその割合が減少することが証明できる. たとえば $n = 2$ の時は円分体の最大実部分体だけが Kummer 対を与える.

さらに簡単な考察により次もわかる.

- (k, m) が Kummer 対であれば, $K = k(\zeta_m) \supsetneq k' \supset k$ をみたす体 k' について (k', m) は Kummer 対である.
- (k, m) が Kummer 対であれば, すべての m の約数 m' について (k, m') は Kummer 対である.

3 証明の概要

証明の詳細は [2] に譲り, ここでは Kummer 対の条件がどのように使われるかだけを述べるにとどめる.

(k, m) を Kummer 対とする. $K = k(\zeta_m), n = [K : k]$ であった. 以後, 簡単に $T = R^{(1)}_{K/k}\mathbb{G}_m$ と書く. (I) より, $\mathrm{End}(T)$ のうち部分拡大から来ていない部分は $\mathbb{Z}[\zeta_n]$ に同型であることが証明できる. したがって T に次数 m の自己準同型が存在するには $\mathbb{Z}[\zeta_n]$ に絶対ノルムが m の元 μ があればよい. これは (IV) で保証される. これが巡回自己準同型になる条件は μ による商環の加法群が巡回群であることが必要十分になる. それを商環の構造定理を使って書き換えたのが (II) である. もう一度 (IV) を使うと $N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}\lambda_i = p_i$ となる $\lambda_i \in \mathbb{Z}[\zeta_n]$ を使って,

$$\mu = \lambda_1 \dots \lambda_r$$

とかける. $\mathrm{Gal}(K/k) = \langle \tau_s \rangle$ と書く. ここで τ_s は $\tau_s(\zeta_m) = \zeta_m^s$ をみたす元で s は $(\mathbb{Z}/m\mathbb{Z})^*$ の中で位数が n の元である. (III) によって λ_i のガロア共役 λ_i' で

$$s \equiv \zeta_n \pmod{\lambda_i'} \tag{2}$$

をみたすものがとれることが証明できる. $\lambda = \prod_{i=1}^{r} \lambda_i'$ とおくと, その構成から λ は次数 m

[*2] $\mathbb{Z}[\zeta_n]$ が単項イデアル整域になるような n は全部で 29 個ある [10, Chapter 11].

の巡回自己準同型になる. (2) から核 $\ker\lambda$ への k の絶対ガロア群の作用は自明になることが証明できる. 完全系列

$$1 \to \ker\lambda \to T \xrightarrow{\lambda} T \to 1.$$

のガロア・コホモロジーをとると,

$$1 \to T(k)/\lambda T(k) \longrightarrow \mathrm{H}^1(k, \ker\lambda) \longrightarrow \ker\left(\lambda : \mathrm{H}^1(k, R^{(1)}_{K/k}\mathbb{G}_m) \to \mathrm{H}^1(k, R^{(1)}_{K/k}\mathbb{G}_m)\right)$$

$$\| $$

$$\mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\bar{k}/k), \ker\lambda)$$

が得られる. また (2) を使った標準的な計算から

$$\mathrm{H}^1(k, R^{(1)}_{K/k}\mathbb{G}_m) \cong k^*/N_{K/k}K^*$$

が得られる. $[K:k] = n$ であるから, 右辺の群は n で消える. $\widehat{\lambda}$ を λ の双対とすると $\widehat{\lambda} \circ \lambda = [m]$ が成り立つ. (II) より m と n は互いに素. よって $\widehat{\lambda} \circ \lambda$ は $\mathrm{H}^1(k, R^{(1)}_{K/k}\mathbb{G}_m)$ 上で単射. よって λ も $\mathrm{H}^1(k, R^{(1)}_{K/k}\mathbb{G}_m)$ 上で単射. したがって

$$\ker\left(\lambda : \mathrm{H}^1(k, R^{(1)}_{K/k}\mathbb{G}_m) \to \mathrm{H}^1(k, R^{(1)}_{K/k}\mathbb{G}_m)\right) = 1$$

がわかり定理が得られる.

4 例

(k, m) を Kummer 対とする. (I) から K/k は巡回拡大である. このとき $R^{(1)}_{K/k}\mathbb{G}_m \cong R_{K/k}\mathbb{G}_m/\mathbb{G}_m$ であり, したがって $\mathbb{P}^{[K:k]-1}$ に埋め込めることが知られている. したがって $R^{(1)}_{K/k}\mathbb{G}_m$ は有理的であり, したがって上記の定理から k の m 次巡回拡大は射影空間の元でパラメーターづけができるわけである. ただし, 高次元の多様体を使っているために, 目的の巡回拡大を記述する方程式は複数になって, それを一つの方程式にまとめることはまだできていない. ただし $n = 2$ の場合には $R^{(1)}_{K/k}\mathbb{G}_m$ は一次元なのでそれが可能である. 先に述べた, 小川, 小松の結果はそれを実行したものになっている. ただしモデルのとり方が標準的ではないので, 以下では標準的なモデルをとって計算を実行してみることにする.

以下では k を円分体 $\mathbb{Q}(\zeta_m)$ の最大実部分体とする. このとき (k, m) は Kummer 対である. 目標は k 上の m 次巡回拡大を与える方程式を具体的に記述することである. $d = (\zeta_m^2 - \zeta_m^{-2})^2 = (\zeta_m + \zeta_m^{-1})^4 - 4(\zeta_m + \zeta_m^{-1})^2 \in k$ とかくと, $K = \mathbb{Q}(\zeta_m) = k(\sqrt{d})$. $R^{(1)}_{K/k}\mathbb{G}_m$ のモデルとして $\mathrm{Spec}\left(k[x_1, x_2]/(x_1^2 - dx_2^2 - 1)\right)$ をとる. m 冪写像 $[m]$ は仮定より $R^{(1)}_{K/k}\mathbb{G}_m$ の次数 m の巡回自己準同型である. $(x_1, x_2) \mapsto (x_1 + x_2\sqrt{d}, x_1 - x_2\sqrt{d})$ で定義される準同

型 $R^{(1)}_{K/k}\mathbb{G}_m \to \mathbb{G}^2_m$ を使って $(f^{(m)}_1, f^{(m)}_2) = [m](x_1, x_2)$ を次のように計算できる.

$$\begin{bmatrix} f^{(m)}_1 \\ f^{(m)}_2 \end{bmatrix} = \begin{bmatrix} 1 & \sqrt{d} \\ 1 & \sqrt{d} \end{bmatrix}^{-1} \begin{bmatrix} (x_1 + x_2\sqrt{d})^m \\ (x_1 - x_2\sqrt{d})^m \end{bmatrix}.$$

これは良く知られた計算で,

$$\begin{aligned} f^{(m)}_1 &= \frac{1}{2}\left((x_1 + \sqrt{d}x_2)^m + (x_1 - \sqrt{d}x_2)^m\right) \\ &= \sum_{i=0}^{\frac{m-1}{2}} \left(\sum_{j=1}^{\frac{m-1}{2}} \binom{m}{2j}\binom{j}{i}(-1)^i x_1^{m-2i} \right), \end{aligned}$$

$$\begin{aligned} f^{(m)}_2 &= \frac{1}{2\sqrt{d}}\left((x_1 + \sqrt{d}x_2)^m - (x_1 - \sqrt{d}x_2)^m\right) \\ &= x_2 \sum_{i=0}^{\frac{m-1}{2}} \left(\sum_{j=1}^{\frac{m-1}{2}} \binom{m}{2j+1}\binom{j}{i}(-1)^i x_1^{m-2i-1} \right) \end{aligned}$$

が得られる. この計算では関係式 $x_1^2 - dx_2^2 = 1$ を使った. これらの多項式は Chebyshev 多項式として知られているもので, 良く知られた漸化式によっても計算できる. $f^{(m)}_2$ の形をみると $k(x_1, x_2) = k(x_1)$ が容易にわかる.

一方, 先に述べた同型 $R_{K/k}\mathbb{G}_m/\mathbb{G}_m \cong R^{(1)}_{K/k}\mathbb{G}_m$ は今の場合 $X \mapsto X^2/N_{K/k}(X)$ で誘導されるから, $[u_1 : u_2] \in \mathbb{P}^1(k)$ に対して

$$\left(\frac{u_1^2 + du_2^2}{u_1^2 - du_2^2}, \frac{2u_1u_2}{u_1^2 - du_2^2} \right) \in R^{(1)}_{K/k}\mathbb{G}_m(k)$$

になる.

以上により $k = \mathbb{Q}(\zeta_m)^+$ 上の m 次巡回拡大はパラメーター $(u_1 : u_2) \in \mathbb{P}^1(k)$ を使って

$$f^{(m)}_1(x) = \frac{u_1^2 + du_2^2}{u_1^2 - du_2^2}$$

で与えられるものでつくされることが結論できる.

参考文献

[1] Taira Honda. Isogenies, rational points and section points of group varieties. *Japan. J. Math.*, 30:84–101, 1960.

[2] Masanari Kida. Kummer theory for norm algebraic tori. 2005. Preprint.

[3] Toru Komatsu. Arithmetic of Rikuna's generic cyclic polynomial and generalization of Kummer theory. *Manuscripta Math.*, 114(3):265–279, 2004.

[4] Boris Kunyavskiĭ and Jean-Jacques Sansuc. Réduction des groupes algébriques commutatifs. *J. Math. Soc. Japan*, 53(2):457–483, 2001.

[5] Serge Lang and John Tate. Principal homogeneous spaces over abelian varieties. *Amer. J. Math.*, 80:659–684, 1958.

[6] Hiroyuki Ogawa. Quadratic reduction of multiplicative group and its applications. *Sūrikaisekikenkyūsho Kōkyūroku*, (1324):217–224, 2003. Algebraic number theory and related topics (Japanese) (Kyoto, 2002).

[7] Takashi Ono. Arithmetic of algebraic tori. *Ann. of Math. (2)*, 74:101–139, 1961.

[8] Kenneth A. Ribet. Kummer theory on extensions of abelian varieties by tori. *Duke Math. J.*, 46(4):745–761, 1979.

[9] V. E. Voskresenskiĭ. *Algebraic groups and their birational invariants*, volume 179 of *Translations of Mathematical Monographs*. American Mathematical Society, Providence, RI, 1998.

[10] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

木田雅成
電気通信大学数学教室
〒182-8585 調布市調布ヶ丘 1-5-1
E-mail: kida@sugaku.e-one.uec.ac.jp
(2004 年 12 月 9 日講演)